

## UNITED STATES DISTRICT COURT

for the  
Western District of Washington

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

HP Touchsmart Computer (SN 3CR8511161), White  
Samsung Galaxy Phone (SN 256691517509643137),  
Seagate Hard Drive (SN 5VJ2X1X5)

Case No. MJ18-045

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):  
The Subject Devices as further described in Attachment A, which is attached hereto and incorporated herein by this reference.

located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, which is attached hereto and incorporated herein by this reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
Title 18, USC § 2252 (a)(2)	Receipt or Distribution of Child Pornography
Title 18, USC § 2252(a)(4)(B)	Possession of Child Pornography
Title 18, USC § 2251(a)	Production of Child Pornography

The application is based on these facts:

See attached Affidavit

- ☒ Continued on the attached sheet.  
☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

  
Applicant's signature

SPECIAL AGENT TOBY LEDGERWOOD, HSI  
Printed name and title

Sworn to before me and signed in my presence.

Date: 2-2-18

City and state: BELLINGHAM, WASHINGTON

  
Judge's signature

PAULA L. MCCANDLIS, U.S. MAGISTRATE JUDGE  
Printed name and title

**ATTACHMENT A**

**Description of Property to be Searched**

The SUBJECT DEVICES, more particularly described below, which are currently in the custody of Homeland Security Investigations in Blaine, Washington:

- a. HP Touchsmart computer Serial Number (SN) 3CR8511161
- b. White Samsung Galaxy Phone SN 256691517509643137
- c. Seagate Hard Drive SN 5VJ2X1X5

**ATTACHMENT B**  
**ITEMS TO BE SEIZED**

The following records, documents, files, or materials, in whatever form, that constitute evidence, instrumentalities, or fruits of violations of 18 U.S.C. § 2251(a) (Production of Child Pornography, 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography), and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography) which may be found at the SUBJECT PREMISES:

1. Any visual depiction of minor(s) engaged in sexually explicit conduct, in any format or media or other evidence of the creation of such visual depictions.

2. Evidence of the installation and use of P2P software, and any associated logs, saved user names and passwords, shared files, and browsing history;

3. Letters, e-mail, text messages, and other correspondence identifying persons transmitting child pornography, or evidencing the transmission of child pornography, through interstate or foreign commerce, including by mail or by computer;

4. All invoices, purchase agreements, catalogs, canceled checks, money order receipts, credit card statements or other documents pertaining to the transportation or purchasing of images of minors engaged in sexually explicit conduct;

5. Any and all address books, names, lists of names, telephone numbers, and addresses of individuals engaged in the transfer, exchange, or sale of child pornography;

6. Any non-digital recording devices and non-digital media capable of storing images and videos.

7. Digital devices and/or their components, which include, but are not limited to:

a. Any digital devices and storage device capable of being used to commit, further, or store evidence of the offense listed above;

b. Any digital devices used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, cameras, printers, encryption devices, and optical scanners;

- 1           c.     Any magnetic, electronic, or optical storage device capable of
- 2 storing data, such as disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, printer or
- 3 memory buffers, smart cards, PC cards, memory sticks, flashdrives, USB/thumb drives,
- 4 camera memory cards, media cards, electronic notebooks, and personal digital assistants;
- 5           d.     Any documentation, operating logs and reference manuals regarding
- 6 the operation of the digital device or software;
- 7           e.     Any applications, utility programs, compilers, interpreters, and other
- 8 software used to facilitate direct or indirect communication with the computer hardware,
- 9 storage devices, or data to be searched;
- 10          f.     Any physical keys, encryption devices, dongles and similar physical
- 11 items that are necessary to gain access to the computer equipment, storage devices or
- 12 data; and
- 13          g.     Any passwords, password files, test keys, encryption codes or other
- 14 information necessary to access the computer equipment, storage devices or data;
- 15        8.     Evidence of who used, owned or controlled any seized digital device(s) at
- 16 the time the things described in this warrant were created, edited, or deleted, such as logs,
- 17 registry entries, saved user names and passwords, documents, and browsing history;
- 18        9.     Evidence of malware that would allow others to control any seized digital
- 19 device(s) such as viruses, Trojan horses, and other forms of malicious software, as well
- 20 as evidence of the presence or absence of security software designed to detect malware;
- 21 as well as evidence of the lack of such malware;
- 22        10.    Evidence of the attachment to the digital device(s) of other storage devices
- 23 or similar containers for electronic evidence;
- 24        11.    Evidence of counter-forensic programs (and associated data) that are
- 25 designed to eliminate data from a digital device;
- 26        12.    Evidence of times the digital device(s) was used;
- 27        13.    Any other ESI from the digital device(s) necessary to understand how the
- 28 digital device was used, the purpose of its use, who used it, and when.

1           14. Records and things evidencing the use of the IP address 73.53.83.83 (the  
2 SUBJECT IP ADDRESS) including:

- 3           a. Routers, modems, and network equipment used to connect  
4 computers to the Internet;  
5           b. Records of Internet Protocol (IP) addresses used;  
6           c. Records of Internet activity, including firewall logs, caches, browser  
7 history and cookies, "bookmarked" or "favorite" web pages, search terms that the user  
8 entered into any Internet search engine, and records of user-typed web addresses.

9  
10 **The seizure of digital devices and/or their components as set forth herein is**  
11 **specifically authorized by this search warrant, not only to the extent that such**  
12 **digital devices constitute instrumentalities of the criminal activity described above,**  
13 **but also for the purpose of the conducting off-site examinations of their contents for**  
14 **evidence, instrumentalities, or fruits of the aforementioned crimes.**  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28



Crimes Against Children (ICAC) Task Force in the Western District of Washington, and work with other federal, state, and local law enforcement personnel in the investigation and prosecution of crimes involving the sexual exploitation of children. I have attended periodic seminars, meetings, and training. I attended the ICAC Undercover Investigations Training Program in Alexandria, Virginia, in June 2014 regarding child exploitation. I also attended the Crimes Against Children Conference in Dallas, Texas, in August 2014, where I received training relating to child exploitation, including training in the Ares Peer to Peer (P2P) file sharing program. In September 2015, I received training in the Emule (P2P) file sharing program. I received a Bachelor of Science degree in Criminal Justice with a minor in Sociology from the University of Missouri-St. Louis.

2. I am submitting this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the three digital devices identified below and in Attachment A (the "SUBJECT DEVICES"), which are currently in the custody of Homeland Security Investigations, for the things specified in Attachment B:

- a. HP Touchsmart computer Serial Number (SN) 3CR8511161
- b. White Samsung Galaxy Phone SN 256691517509643137;
- c. Seagate Hard Drive SN 5VJ2X1X5

3. The warrant would authorize a search of the SUBJECT DEVICES and forensic examination, for the purpose of identifying electronically stored data as particularly described in Attachment B, for evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2251(a) (Production of Child Pornography), 18 U.S.C. §§ 2252(a)(2) (Receipt or Distribution of Child Pornography), and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography).

4. The facts set forth in this Affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; review of documents and records related to this investigation; communications with others who have personal knowledge

1 of the events and circumstances described herein; and information gained through my  
2 training and experience.

3 5. Because this affidavit is submitted for the limited purpose of establishing  
4 probable cause in support of the application for a search warrant, it does not set forth  
5 each and every fact that I or others have learned during the course of this investigation. I  
6 have set forth only the facts that I believe are relevant to the determination of probable  
7 cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C.  
8 § 2251(a) (Production of Child Pornography), 18 U.S.C. § 2252(a)(2) (Receipt or  
9 Distribution of Child Pornography), and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child  
10 Pornography), will be found on the SUBJECT DEVICES.

## 11 II. DEFINITIONS

12 6. The following definitions apply to this Affidavit:

### 13 Internet Service Providers

14 a. "Internet Service Providers" (ISPs), as used herein, are commercial  
15 organizations that are in business to provide individuals and businesses access to the  
16 internet. ISPs provide a range of functions for their customers including access to the  
17 Internet, web hosting, email, remote storage, and co-location of computers and other  
18 communications equipment. ISPs can offer a range of options in providing access to the  
19 Internet including telephone based dial up, broadband based access via digital subscriber  
20 line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs  
21 typically charge a fee based upon the type of connection and volume of data, called  
22 bandwidth, which the connection supports. Many ISPs assign each subscriber an account  
23 name – a user name or screen name, an "email address," an email mailbox, and a  
24 personal password selected by the subscriber. By using a computer equipped with a  
25 modem, the subscriber can establish communication with an ISP over a telephone line,  
26 through a cable system or via satellite, and can access the Internet by using his or her  
27 account name and personal password. ISPs maintain records pertaining to their  
28 subscribers (regardless of whether those subscribers are individuals or entities). These



records may include account application information, subscriber and billing information, account access information (often times in the form of log files), email communications, information concerning content uploaded and/or stored on or via the ISP's servers.

#### Internet Protocol (IP) Addresses

b. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer connected to the Internet must be assigned an IP address so that the Internet traffic sent from, and directed to, that computer may be properly directed from its source to its destination. Most ISPs control the range of IP addresses.

### **III. The CyberTip and ESP Rabbit**

7. This investigation arose from a CyberTip submitted to the National Center for Missing and Exploited Children (NCMEC). NCMEC is a private non-profit organization operating under a Congressional mandate to act as the nation's law enforcement clearing house for information concerning online child sexual exploitation. In partial fulfillment of that mandate, NCMEC operates a CyberTip line, a resource for reporting online crimes against children. Electronic Service Providers (ESPs) report to NCMEC, via the CyberTip line, whenever they discover that a subscriber has violated the terms of service and/or their services have been used to transmit child pornography over the Internet.

8. The CyberTip giving rise to this investigation came from ESP Rabbit.

According to the ESP itself,

Rabbit is about sharing your everyday. Watch your favorite shows with your friends, without being in the same room (or even the same city!). Collaborate with your coworkers when you're all on the road. Shop together for a birthday present for Mom, then sing her "happy birthday" with family far away. The possibilities are endless. Rabbit started with an idea: people sharing experiences online from wherever they are. We began with an app for Mac in February 2013. Then in August 2014, we launched a web-based version of Rabbit. In February 2-15, we were named one of the Top 10 Most Innovative Companies in Video by Fast

1 Company. And in October 2015, we launched an app for iOS. But this is only the  
2 start: we've got big plans.

#### 3 IV. STATEMENT OF PROBABLE CAUSE

4 9. In December 2017, Homeland Security Investigations (HSI) Blaine,  
5 Washington received CyberTip report #25955849 from the Seattle Internet Crimes  
6 Against Children (ICAC) Task Force. The report indicated the ESP, Rabbit, reported that  
7 one of its users uploaded several images of suspected child pornography to its website.  
8 According to the CyberTip, the user was named, Lovr E, and has a screen/user name,  
9 Lovr1. The report also stated that the IP address of the device that uploaded these images  
10 of suspected child pornography was 73.53.83.83 (the SUBJECT IP ADDRESS).  
11 According to the CyberTip, that user uploaded approximately thirteen images depicting  
12 suspected child pornography between November 26, 2017, and November 27, 2017, from  
13 the SUBJECT IP ADDRESS. Before submitting the CyberTip, employee(s) of Rabbit  
14 examined each of these images of suspected of child pornography.

15 10. I have reviewed these images of suspected child pornography and describe  
16 each below:

17 **Filename: Lovr1\_20171126\_2.png**

18 This color image depicts a prepubescent female (hereinafter the "child victim").  
19 The child victim is nude and laying on her back visible from her waist to her  
20 thighs. The child victim's legs are spread apart and her unclothed genital area is  
21 the focal point of the image. An orange carrot is inserted into her vagina by what  
22 appears to be an adult's hand. The child victim has no visible pubic hair and is  
23 very small in stature. The child victim appears to be approximately 5 to 6 years  
24 old.

25 **Filename: Lovr1\_20171126\_1.png**

26 This color image depicts a prepubescent female (hereinafter the "child victim").  
27 The child victim is completely nude and laying on her back. She is fully visible.  
28 The child is lying on a blue blanket with black squares. The child's legs are  
spread apart. A hairy adult arm and hand is holding a white sex toy in front of her  
vagina. There appears to be a shiny lubricant around the child victim's vaginal  
area. The child victim's vagina is not exposed due to the sex toy being placed in  
front of or on it. The child victim's breasts are exposed. She has no visible pubic  
hair, lacks muscular and breast development and is very small in stature. The  
child victim appears to be approximately 5-6 years old.

11. Rabbit also provided several pages of chats from the user Lovr1. On November 26, 2017, and November 27, 2017, Lovr1 had a conversation with an unknown user discussing having an “ex’s daughter” who appears to be a child named “[MV]”. During this chat, Lovr1 states, “i still get my ex’s daughter all the time on weekends, [S.] is always like, oh shes a cutie”, “its fucking cute seeing her cuddle with her, seeing [MV] wrap her legs around [S.], its soooo hot to think about”. Later in the conversation, Lovr1 states: “mmm, could use her little sisters feet to rub on [MV’s] pussy:)”, “mmmm god yes, i love kissing [MV’s] feet”, “god why is little girl pussy the hottest thing on earth”, “i bet its even more amazing making a little girl cummmm”, “coat that ball with KY and get [MV] and her little sister on it together!!!”, “god I want [MV] to be the one to teach them aboutr their pussies !!!”.

12. In addition to the above messages discussing the sexual abuse of MV, there is a series of messages in which Lovr1 recounts taking MV to a hotel over a weekend and then sends images purportedly of MV, in which MV’s breasts and vagina are exposed. These images were among the images flagged (and viewed) by Rabbit and included with the CyberTip. They depict a prepubescent girl between six and nine years old next to a bed, in what appears to be a hotel room.

13. A query of a publicly available database revealed the SUBJECT IP ADDRESS belonged to ISP Comcast Communications.

14. On December 06, 2017, a Department of Homeland Security (DHS) administrative summons’ was submitted to Comcast requesting subscriber information for the SUBJECT IP ADDRESS during the date and time the subject image files were uploaded.

15. On December 08, 2017, Comcast provided the requested information. During the date and time the subject image files were uploaded, the SUBJECT IP ADDRESS was assigned to C.P. at the residence located at 8575 Vinup Rd, Apt B, Lynden, Washington (the SUBJECT PREMISES). Comcast revealed the IP History of the SUBJECT IP ADDRESS to have a lease grant date and time of October 20, 2017, at

1 19:56:45 UTC and a lease expiration of December 06, 2017, at 23:01:48 UTC. The  
2 SUBJECT IP ADDRESS is leased to C.P. with account number ending in 7795.

3 16. Intelligence Research Specialist/Computer Forensic Analyst (IRS/CFA)  
4 Gillie conducted records checks via a law enforcement database and found that C.P.  
5 (DOB XX/XX/1989) has been associated with the SUBJECT PREMISES since June  
6 2017. I conducted a search via the Washington State Department of Licensing  
7 (WSDOL) and learned that C.P. has a 2007 Hyundai, registered at the SUBJECT  
8 PREMISES. WSDOL also revealed C.P. was issued a Washington State driver's license  
9 on September 12, 2017, with the SUBJECT PRIMISES listed as her address.

10 17. On December 8, 2017, at approximately 3:30 p.m., SA Jesse Miller  
11 conducted surveillance of the SUBJECT PREMISES and observed the following vehicle  
12 parked in the driveway: Hyundai bearing Washington State license plate BGV7348.  
13 Records checks revealed that the vehicles are registered to C.P. at the SUBJECT  
14 PREMISES.

15 18. On December 14, 2017, I obtained a federal search warrant for the  
16 SUBJECT PREMISES from Judge Paula L. McCandlis of the United States District  
17 Court for the Western District of Washington. A team of federal and local law  
18 enforcement officers served this warrant just after 5:00 p.m. the same day.

19 19. Upon encountering BARTELS inside the SUBJECT PREMISES, I  
20 informed him that we had a warrant to search the apartment. I conducted a search of  
21 BARTELS and found a cellular phone. After he used the restroom, BARTELS  
22 accompanied me to my government car along with Det. Pauline Renick. I asked  
23 BARTELS if we could record our conversation with him, and he declined. I read  
24 BARTELS his Miranda rights, and BARTELS said he understood them. I explained to  
25 BARTELS that we obtained a search warrant to search his home and that we were  
26 searching for evidence of child pornography. BARTELS initially stated he did not know  
27 anything about child pornography or Rabbit. I asked BARTELS about a child named  
28 "MV" and her mother "S." I asked if these were fictitious people, and he said they were.

1 I explained to BARTELS that I would need to talk to his girlfriend and friends in order to  
2 figure out if he were the person making child pornography and sharing it over Rabbit.  
3 Our interview with BARTELS continued through the course of the evening. At several  
4 points, BARTELS inquired whether he should speak with an attorney. Each time he  
5 made such an inquiry, he was advised that the decision to ask for an attorney was his to  
6 make.

7 20. Just before 6:00 p.m., Det. Renick and I paused our conversation with  
8 BARTELS so we could interview other witnesses. Shortly thereafter, BARTELS drank  
9 four twelve ounce Rolling Rock beers in quick succession.

10 21. Det. Renick and I first conducted a recorded interview of C.P. I explained  
11 to C.P. why we were at her home. I showed C.P. several images that were uploaded by  
12 Lovr1, including the images taken in a hotel room described above. She identified the  
13 prepubescent girl pictured in the images as CV1. She identified a second prepubescent  
14 minor pictured in some of these images as CV1's sister. Det. Renick and I then  
15 interviewed MW at approximately 7:37 p.m. MW likewise confirmed the identities of  
16 CV1 and her sister after being shown the images shown to C.P.

17 22. Upon completing the interview with MW, Det. Renick approached  
18 BARTELS, who was in the kitchen of the SUBJECT PREMISES. Det. Renick asked  
19 BARTELS if he had thought about what had been happening that evening, and he said he  
20 had. She explained to him that she had just interviewed MW, who had identified CV1,  
21 her sister, and the hotel room pictured in the images uploaded by Lovr1. Det. Renick  
22 asked BARTELS if he wanted to talk about what was going on, and he said yes.

23 23. BARTELS again declined a request to record the conversation and simply  
24 stated that he was aware whatever he said could be used against him. BARTELS asked  
25 Det. Renick what she wanted to know. Det. Renick told BARTELS that she just wanted  
26 to know the truth about what was going on. She explained that it was not a matter of  
27 whether or not the viewing and production of the child pornography happened but rather  
28 why. BARTELS stated that he was molested by his mother as a child. He could not say

1 when it started because he was very young, and he could not recall when it stopped as he  
2 had tried to put it out of his mind. He continued that he never sought help for the abuse  
3 and that he is not sure why he started looking at child pornography but he did in fact do  
4 so. He explained that child pornography was like a drug and that he could not quit  
5 viewing it.

6 24. When confronted with the images of CV1 taken in the hotel room,  
7 BARTELS acknowledged taking the photos while in the room with CV1. He explained  
8 he had been staying in a hotel room in Bremerton, Washington, with CV1, CV1's sister,  
9 CV1's mother, and MW. BARTELS admitted that he had taken these photos of CV1  
10 undressing and in the nude and then traded them with others on Rabbit. When Det.  
11 Renick asked him how many times he had traded these images, BARTELS said he was  
12 unsure but guessed it to be three to five times. BARTELS said he had taken the photos  
13 with his cell phone. BARTELS also acknowledged being the Rabbit user that was the  
14 subject of the CyberTip and confirmed engaging in the chats described above.

15 25. BARTELS was arrested and transported to the Bellingham police  
16 department just after 10:00 p.m. While being transported by Special Agent Shaun Smith,  
17 BARTELS stated that he was glad he was caught because it felt like a big weight had  
18 been lifted.

19 26. At approximately 10:45 p.m., Det. Renick and I asked BARTELS if he  
20 would continue speaking with us. He again declined our request to record our  
21 conversation but agreed to speak further. BARTELS explained that he took the  
22 photographs of CV1 undressing at a hotel in Bremerton, which he believed might be the  
23 Quality Inn. He stated he took approximately five photographs of CV1 without her  
24 knowledge or the knowledge of anyone else in the room. BARTELS also stated he  
25 captured a webcam video of CV1 in her underwear on at least one other occasion while  
26 he was chatting with another individual online. BARTELS stated these were the only  
27 two times he had ever attempted to capture a pornographic image or video of CV1.  
28

1       27. After confirming that he had shared images of CV1 using Rabbit and  
2 another forum, I asked BARTELS why he started taking pornographic pictures of CV1.  
3 He explained, "Because of chats and talking to people, like a heroin addict once you take  
4 a hit."

5       28. Det. Renick asked BARTELS if he ever thought he would get into trouble  
6 and he said yes. He explained that anytime he was talking with someone online, he  
7 thought he could be talking to police.

8       29. BARTELS said he looked at child pornography a couple of times a month  
9 and masturbates to it "maybe 2 outta 20 times." He stated that he possessed a couple  
10 hundred images and videos of child pornography.

11       30. Among the items seized from the SUBJECT PREMISES was a laptop  
12 computer that belongs to BARTELS. During the forensic preview of this device, CFA  
13 Tom Gillie was able to confirm that it contained several of the same images that were the  
14 subject of the Rabbit CyberTip.

15       31. Forensic analysis of the devices seized from the SUBJECT PREMISES has  
16 thus far revealed the presence of thousands of images and videos of minors engaged in  
17 sexually explicit conduct.

18       32. On December 15, 2017, I transported BARTELS from the Whatcom  
19 County jail to the federal courthouse in Seattle. I advised him that I was using a  
20 recording device to record our conversation on the way down to Seattle. I reminded him  
21 of his *Miranda* rights, and he stated he understood them. During our conversation, he  
22 confirmed nearly all of the information he provided the previous evening as well as  
23 stating his desire to apologize for what he done to CV1.

24       33. A Grand Jury sitting in the Western District of Washington has returned an  
25 indictment charging BARTELS with one count each of Production of Child Pornography  
26 in violation of 18 U.S.C. § 2251(a), Distribution of Child Pornography in violation of 18  
27 U.S.C. § 2252(a)(2), and Possession of Child Pornography in violation of 18 U.S.C.  
28 § 2252(a)(4)(B).



34. On December 18, 2017, CFA Gillie and I interviewed N.F. and R.F. of Ferndale, Washington. N.F. stated BARTELS moved into the residence on or about December 28, 2016, and left the residence in April of 2017. N.F. stated her ten-year-old niece disclosed that BARTELS had been inappropriately touching her nine-year-old cousin.

35. N.F. stated she called 911 and reported the alleged incident to police. N.F. stated she was instructed by police to take her family and leave the residence without disclosing to BARTELS the reason. N.F. stated she left with her family for two weeks. N.F. stated BARTELS attempted to make contact with her regarding why she left, and she did not engage in conversation with BARTELS. N.F. stated a sergeant with Ferndale police called BARTELS and requested BARTELS come in for an interview. According to N.F., BARTELS did not show up for the interview and abandoned all his property at her residence, including two of the SUBJECT DEVICES—the Samsung cell phone and HP Touchsmart computer. N.F. stated she was told BARTELS left the Whatcom County area.

36. After BARTELS left the area and abandoned his property, N.F. and her family returned to their residence. R.F. said that, due to the allegations made against BARTELS, he decided to clone BARTELS's computer (the HP Touchsmart) using a Seagate Hard Drive, the third of the SUBJECT DEVICES. The hard drive has a label made by R.F. that says, "CLONE OF JAMIE'S COMPUTER". It is my understanding that R.F. has the technical expertise to clone a computer based on his employment.

37. N.F. and R.F. allowed CFA Gillie and I to take the SUBJECT DEVICES for forensic analysis. Because BARTELS abandoned the HP Touchsmart and Samsung cell phone, I do not believe a warrant is required to seize and search the SUBJECT DEVICES. I am nonetheless seeking this warrant out of an abundance of caution.

## VI. TECHNICAL BACKGROUND

38. Based on my training and experience, when an individual communicates through the Internet, the individual leaves an IP address which identifies the individual



1 user by account and ISP (as described above). When an individual is using the Internet,  
2 the individual's IP address is visible to administrators of websites they visit. Further, the  
3 individual's IP address is broadcast during most Internet file and information exchanges  
4 that occur.

5 39. Based on my training and experience, I know that most ISPs provide only  
6 one IP address for each residential subscription. I also know that individuals often use  
7 multiple digital devices within their home to access the Internet, including desktop and  
8 laptop computers, tablets, and mobile phones. A device called a router is used to connect  
9 multiple digital devices to the Internet via the public IP address assigned (to the  
10 subscriber) by the ISP. A wireless router performs the functions of a router but also  
11 includes the functions of a wireless access point, allowing (wireless equipped) digital  
12 devices to connect to the Internet via radio waves, not cables. Based on my training and  
13 experience, today many residential Internet customers use a wireless router to create a  
14 computer network within their homes where users can simultaneously access the Internet  
15 (with the same public IP address) with multiple digital devices.

16 40. Based on my training and experience and information provided to me by  
17 computer forensic agents, I know that data can quickly and easily be transferred from one  
18 digital device to another digital device. Data can be transferred from computers or other  
19 digital devices to internal and/or external hard drives, tablets, mobile phones, and other  
20 mobile devices via a USB cable or other wired connection. Data can also be transferred  
21 between computers and digital devices by copying data to small, portable data storage  
22 devices including USB (often referred to as "thumb") drives, memory cards (Compact  
23 Flash, SD, microSD, etc.) and memory card readers, and optical discs (CDs/DVDs).

24 41. As outlined above, residential Internet users can simultaneously access the  
25 Internet in their homes with multiple digital devices. Also explained above is how data  
26 can quickly and easily be transferred from one digital device to another through the use  
27 of wired connections (hard drives, tablets, mobile phones, etc.) and portable storage  
28 devices (USB drives, memory cards, optical discs). Therefore, a user could access the

1 Internet using their assigned public IP address, receive, transfer or download data, and  
2 then transfer that data to other digital devices which may or may not have been connected  
3 to the Internet during the date and time of the specified transaction.

4 42. Based on my training and experience, I have learned that the computer's  
5 ability to store images and videos in digital form makes the computer itself an ideal  
6 repository for child pornography. The size of hard drives used in computers (and other  
7 digital devices) has grown tremendously within the last several years. Hard drives with  
8 the capacity of four (4) terabytes (TB) are not uncommon. These drives can store  
9 thousands of images and videos at very high resolution.

10 43. Based on my training and experience, collectors and distributors of child  
11 pornography also use online resources to retrieve and store child pornography, including  
12 services offered by companies such as Google, Yahoo, Apple, and Dropbox, among  
13 others. The online services allow a user to set up an account with a remote computing  
14 service that provides email services and/or electronic storage of computer files in any  
15 variety of formats. A user can set up an online storage account from any computer with  
16 access to the Internet. Evidence of such online storage of child pornography is often  
17 found on the user's computer. Even in cases where online storage is used, however,  
18 evidence of child pornography can be found on the user's computer in most cases.

19 44. As is the case with most digital technology, communications by way of  
20 computer can be saved or stored on the computer used for these purposes. Storing this  
21 information can be intentional, i.e., by saving an email as a file on the computer or saving  
22 the location of one's favorite websites in, for example, "bookmarked" files. Digital  
23 information can also be retained unintentionally, e.g., traces of the path of an electronic  
24 communication may be automatically stored in many places (e.g., temporary files or ISP  
25 client software, among others). In addition to electronic communications, a computer  
26 user's Internet activities generally leave traces or "footprints" and history files of the  
27 browser application used. A forensic examiner often can recover evidence suggesting  
28 whether a computer contains wireless software, and when certain files under investigation

1 | were uploaded or downloaded. Such information is often maintained indefinitely until  
2 | overwritten by other data.

3 |       45. Based on my training and experience, I have learned that producers of child  
4 | pornography can produce image and video digital files from the average digital camera,  
5 | mobile phone, or tablet. These files can then transferred from the mobile device to a  
6 | computer or other digital device, using the various methods described above. The digital  
7 | files can then be stored, manipulated, transferred, or printed directly from a computer or  
8 | other digital device. Digital files can also be edited in ways similar to those by which a  
9 | photograph may be altered; they can be lightened, darkened, cropped, or otherwise  
10 | manipulated. As a result of this technology, it is relatively inexpensive and technically  
11 | easy to produce, store, and distribute child pornography. In addition, there is an added  
12 | benefit to the child pornographer in that this method of production is a difficult trail for  
13 | law enforcement to follow.

14 |       46. As part of my training and experience, I have become familiar with the  
15 | structure of the Internet, and I know that connections between computers on the Internet  
16 | routinely cross state and international borders, even when the computers communicating  
17 | with each other are in the same state. Individuals and entities use the Internet to gain  
18 | access to a wide variety of information; to send information to, and receive information  
19 | from, other individuals; to conduct commercial transactions; and to communicate via  
20 | email.

21 |       47. Based on my training and experience, I know that cellular mobile phones  
22 | (often referred to as "smart phones") have the capability to access the Internet and store  
23 | information, such as images and videos. As a result, an individual using a smart phone  
24 | can send, receive, and store files, including child pornography, without accessing a  
25 | personal computer or laptop. An individual using a smart phone can also easily connect  
26 | the device to a computer or other digital device, via a USB or similar cable, and transfer  
27 | data files from one digital device to another.

1        48. As set forth herein and in Attachment B to this Affidavit, I seek permission  
2 to search for and seize evidence, fruits, and instrumentalities of the above-referenced  
3 crimes that might be found on the SUBJECT DEVICES in whatever form they are found.  
4 It has been my experience that individuals involved in child pornography often prefer to  
5 store images of child pornography in electronic form. The ability to store images of child  
6 pornography in electronic form makes digital devices, examples of which are enumerated  
7 in Attachment B to this Affidavit, an ideal repository for child pornography because the  
8 images can be easily sent or received over the Internet. As a result, one form in which  
9 these items may be found is as electronic evidence stored on a digital device.

10        49. Based upon my knowledge, experience, and training in child pornography  
11 investigations, and the training and experience of other law enforcement officers with  
12 whom I have had discussions, I know that there are certain characteristics common to  
13 individuals who have a sexualized interest in children and depictions of children:

14            a. They may receive sexual gratification, stimulation, and satisfaction  
15 from contact with children; or from fantasies they may have viewing children engaged in  
16 sexual activity or in sexually suggestive poses, such as in person, in photographs, or other  
17 visual media; or from literature describing such activity.

18            b. They may collect sexually explicit or suggestive materials in a  
19 variety of media, including photographs, magazines, motion pictures, videotapes, books,  
20 slides, and/or drawings or other visual media. Such individuals often times use these  
21 materials for their own sexual arousal and gratification. Further, they may use these  
22 materials to lower the inhibitions of children they are attempting to seduce, to arouse the  
23 selected child partner, or to demonstrate the desired sexual acts. These individuals may  
24 keep records, to include names, contact information, and/or dates of these interactions, of  
25 the children they have attempted to seduce, arouse, or with whom they have engaged in  
26 the desired sexual acts.

27            c. They often maintain any "hard copies" of child pornographic  
28 material that is, their pictures, films, video tapes, magazines, negatives, photographs,

1 correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of  
2 their home or some other secure location. These individuals typically retain these “hard  
3 copies” of child pornographic material for many years, as they are highly valued.

4 d. Likewise, they often maintain their child pornography collections  
5 that are in a digital or electronic format in a safe, secure and private environment, such as  
6 a computer and surrounding area. These collections are often maintained for several  
7 years and are kept close by, often at the individual’s residence or some otherwise easily  
8 accessible location, to enable the owner to view the collection, which is valued highly.  
9 They also may opt to store the contraband in cloud accounts. Cloud storage is a model of  
10 data storage where the digital data is stored in logical pools, the physical storage can span  
11 multiple servers, and often locations, and the physical environment is typically owned  
12 and managed by a hosting company. Cloud storage allows the offender ready access to  
13 the material from any device that has an Internet connection, worldwide, while also  
14 attempting to obfuscate or limit the criminality of possession as the material is stored  
15 remotely and not on the offender’s device.

16 e. They also may correspond with and/or meet others to share  
17 information and materials; rarely destroy correspondence from other child pornography  
18 distributors/collectors; conceal such correspondence as they do their sexually explicit  
19 material; and often maintain lists of names, addresses, and telephone numbers of  
20 individuals with whom they have been in contact and who share the same interests in  
21 child pornography.

22 f. They generally prefer not to be without their child pornography for  
23 any prolonged time period. This behavior has been documented by law enforcement  
24 officers involved in the investigation of child pornography throughout the world.

25 g. E-mail itself provides a convenient means by which individuals can  
26 access a collection of child pornography from any computer, at any location with Internet  
27 access. Such individuals therefore do not need to physically carry their collections with  
28 them but rather can access them electronically. Furthermore, these collections can be

1 stored on email "cloud" servers, which allow users to store a large amount of material at  
2 no cost, without leaving any physical evidence on the users' computer(s).

3 50. In addition to offenders who collect and store child pornography, law  
4 enforcement has encountered offenders who obtain child pornography from the internet,  
5 view the contents and subsequently delete the contraband, often after engaging in self-  
6 gratification. In light of technological advancements, increasing Internet speeds and  
7 worldwide availability of child sexual exploitative material, this phenomenon offers the  
8 offender a sense of decreasing risk of being identified and/or apprehended with quantities  
9 of contraband. This type of consumer is commonly referred to as a 'seek and delete'  
10 offender, knowing that the same or different contraband satisfying their interests remain  
11 easily discoverable and accessible online for future viewing and self-gratification. I  
12 know that, regardless of whether a person discards or collects child pornography he/she  
13 accesses for purposes of viewing and sexual gratification, evidence of such activity is  
14 likely to be found on computers and related digital devices, including storage media, used  
15 by the person. This evidence may include the files themselves, logs of account access  
16 events, contact lists of others engaged in trafficking of child pornography, backup files,  
17 and other electronic artifacts that may be forensically recoverable.

18 51. Given the above-stated facts and based on my knowledge, training and  
19 experience, along with my discussions with other law enforcement officers who  
20 investigate child exploitation crimes, I believe that BARTELS likely has a sexualized  
21 interest in children and depictions of children. I therefore believe that evidence of child  
22 pornography is likely to be found on the SUBJECT DEVICES.

23 52. Based on my training and experience, and that of computer forensic agents  
24 that I work and collaborate with on a daily basis, I know that every type and kind of  
25 information, data, record, sound or image can exist and be present as electronically stored  
26 information on any of a variety of computers, computer systems, digital devices, and  
27 other electronic storage media. I also know that electronic evidence can be moved easily  
28 from one digital device to another.



1       53. Based on my training and experience, and my consultation with computer  
2 forensic agents who are familiar with searches of computers, I know that in some cases  
3 the items set forth in Attachment B may take the form of files, documents, and other data  
4 that is user-generated and found on a digital device. In other cases, these items may take  
5 the form of other types of data - including in some cases data generated automatically by  
6 the devices themselves.

7       54. Based on my training and experience, and my consultation with computer  
8 forensic agents who are familiar with searches of computers, I believe there is probable  
9 cause to believe that the items set forth in Attachment B will be stored in those digital  
10 devices for a number of reasons, including but not limited to the following:

11           a. Once created, electronically stored information (ESI) can be stored  
12 for years in very little space and at little or no cost. A great deal of ESI is created, and  
13 stored, moreover, even without a conscious act on the part of the device operator. For  
14 example, files that have been viewed via the Internet are sometimes automatically  
15 downloaded into a temporary Internet directory or "cache," without the knowledge of the  
16 device user. The browser often maintains a fixed amount of hard drive space devoted to  
17 these files, and the files are only overwritten as they are replaced with more recently  
18 viewed Internet pages or if a user takes affirmative steps to delete them. This ESI may  
19 include relevant and significant evidence regarding criminal activities, but also, and just  
20 as importantly, may include evidence of the identity of the device user, and when and  
21 how the device was used. Most often, some affirmative action is necessary to delete ESI.  
22 And even when such action has been deliberately taken, ESI can often be recovered,  
23 months or even years later, using forensic tools.

24           b. Wholly apart from data created directly (or indirectly) by user-  
25 generated files, digital devices - in particular, a computer's internal hard drive - contain  
26 electronic evidence of how a digital device has been used, what it has been used for, and  
27 who has used it. This evidence can take the form of operating system configurations,  
28 artifacts from operating systems or application operations, file system data structures, and

1 virtual memory "swap" or paging files. Computer users typically do not erase or delete  
2 this evidence, because special software is typically required for that task. However, it is  
3 technically possible for a user to use such specialized software to delete this type of  
4 information - and, the use of such special software may itself result in ESI that is relevant  
5 to the criminal investigation. HSI agents in this case have consulted on computer  
6 forensic matters with law enforcement officers with specialized knowledge and training  
7 in computers, networks, and Internet communications. In particular, to properly retrieve  
8 and analyze electronically stored (computer) data, and to ensure accuracy and  
9 completeness of such data and to prevent loss of the data either from accidental or  
10 programmed destruction, it is necessary to conduct a forensic examination of the  
11 computers. To effect such accuracy and completeness, it may also be necessary to  
12 analyze not only data storage devices, but also peripheral devices which may be  
13 interdependent, the software to operate them, and related instruction manuals containing  
14 directions concerning operation of the computer and software.

## 15 **VII. SEARCH AND/OR SEIZURE OF DIGITAL DEVICES**

16 55. In addition, based on my training and experience and that of computer  
17 forensic agents that I work and collaborate with on a daily basis, I know that in most  
18 cases it is impossible to successfully conduct a complete, accurate, and reliable search for  
19 electronic evidence stored on a digital device during the physical search of a search site  
20 for a number of reasons, including but not limited to the following:

21 a. Technical Requirements: Searching digital devices for criminal  
22 evidence is a highly technical process requiring specific expertise and a properly  
23 controlled environment. The vast array of digital hardware and software available  
24 requires even digital experts to specialize in particular systems and applications, so it is  
25 difficult to know before a search which expert is qualified to analyze the particular  
26 system(s) and electronic evidence found at a search site. As a result, it is not always  
27 possible to bring to the search site all of the necessary personnel, technical manuals, and  
28 specialized equipment to conduct a thorough search of every possible digital



1 device/system present. In addition, electronic evidence search protocols are exacting  
2 scientific procedures designed to protect the integrity of the evidence and to recover even  
3 hidden, erased, compressed, password-protected, or encrypted files. Since ESI is  
4 extremely vulnerable to inadvertent or intentional modification or destruction (both from  
5 external sources or from destructive code embedded in the system such as a "booby  
6 trap"), a controlled environment is often essential to ensure its complete and accurate  
7 analysis.

8           b.     Volume of Evidence: The volume of data stored on many digital  
9 devices is typically so large that it is impossible to search for criminal evidence in a  
10 reasonable period of time during the execution of the physical search of a search site. A  
11 single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A  
12 single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000  
13 double-spaced pages of text. Computer hard drives are now being sold for personal  
14 computers capable of storing up to four terabytes (4,000 gigabytes of data.) Additionally,  
15 this data may be stored in a variety of formats or may be encrypted (several new  
16 commercially available operating systems provide for automatic encryption of data upon  
17 shutdown of the computer).

18           c.     Search Techniques: Searching the ESI for the items described in  
19 Attachment B may require a range of data analysis techniques. In some cases, it is  
20 possible for agents and analysts to conduct carefully targeted searches that can locate  
21 evidence without requiring a time-consuming manual search through unrelated materials  
22 that may be commingled with criminal evidence. In other cases, however, such  
23 techniques may not yield the evidence described in the warrant, and law enforcement  
24 personnel with appropriate expertise may need to conduct more extensive searches, such  
25 as scanning areas of the disk not allocated to listed files, or peruse every file briefly to  
26 determine whether it falls within the scope of the warrant.

27           56.     Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal  
28 Rules of Criminal Procedure, the warrant I am applying for will permit imaging or

1 otherwise copying all data contained on the SUBJECT DEVICES, and will specifically  
2 authorize a review of the media or information consistent with the warrant.

3 57. In accordance with the information in this affidavit, law enforcement  
4 personnel will execute the search of the SUBJECT DEVICE/S pursuant to this warrant as  
5 follows:


6 58. Securing the Data: In order to examine the ESI in a forensically sound  
7 manner, law enforcement personnel with appropriate expertise will attempt to produce a  
8 complete forensic image, if possible and appropriate, of the SUBJECT DEVICES. Law  
9 enforcement will only create an image of data physically present on or within the  
10 SUBJECT DEVICE/S. Creating an image of the SUBJECT DEVICE/S will not result in  
11 access to any data physically located elsewhere. However, SUBJECT DEVICES that  
12 have previously connected to devices at other locations may contain data from those  
13 other locations.

14 59. Searching the Forensic Images: Searching the forensic images for the items  
15 described in Attachment B may require a range of data analysis techniques. In some  
16 cases, it is possible for agents and analysts to conduct carefully targeted searches that can  
17 locate evidence without requiring a time-consuming manual search through unrelated  
18 materials that may be commingled with criminal evidence. In other cases, however, such  
19 techniques may not yield the evidence described in the warrant, and law enforcement  
20 may need to conduct more extensive searches to locate evidence that falls within the  
21 scope of the warrant. The search techniques that will be used will be only those  
22 methodologies, techniques and protocols as may reasonably be expected to find, identify,  
23 segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to  
24 this affidavit.

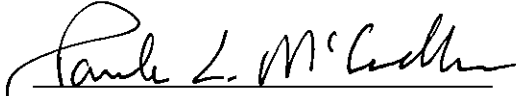
## 25 VIII. CONCLUSION

26 60. Based on the foregoing, I believe there is probable cause that evidence,  
27 fruits, and instrumentalities of violations of 18 U.S.C. § 2251(a) (Production of Child  
28 Pornography), 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography),

1 and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography), are located on/in the  
2 SUBJECT DEVICES as more fully described in Attachment A to this Affidavit, I  
3 therefore request that the court issue a warrant authorizing a search of the SUBJECT  
4 DEVICES specified in Attachment A for the items more fully described in Attachment B.  
5  
6  
7

  
Toby Ledgerwood, Affiant  
Special Agent  
Department of Homeland Security  
Homeland Security Investigations

11 SUBSCRIBED and SWORN to before me this 2<sup>nd</sup> day of February, 2018.  
12  
13

  
PAULA L. MCCANDLIS  
United States Magistrate Judge  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**ATTACHMENT A**

**Description of Property to be Searched**

The SUBJECT DEVICES, more particularly described below, which are currently in the custody of Homeland Security Investigations in Blaine, Washington:

- a. HP Touchsmart computer Serial Number (SN) 3CR8511161
- b. White Samsung Galaxy Phone SN 256691517509643137
- c. Seagate Hard Drive SN 5VJ2X1X5

**ATTACHMENT B****ITEMS TO BE SEIZED**

The following records, documents, files, or materials, in whatever form, that constitute evidence, instrumentalities, or fruits of violations of 18 U.S.C. § 2251(a) (Production of Child Pornography, 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography), and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography) which may be found at the SUBJECT PREMISES:

1. Any visual depiction of minor(s) engaged in sexually explicit conduct, in any format or media or other evidence of the creation of such visual depictions.

2. Evidence of the installation and use of P2P software, and any associated logs, saved user names and passwords, shared files, and browsing history;

3. Letters, e-mail, text messages, and other correspondence identifying persons transmitting child pornography, or evidencing the transmission of child pornography, through interstate or foreign commerce, including by mail or by computer;

4. All invoices, purchase agreements, catalogs, canceled checks, money order receipts, credit card statements or other documents pertaining to the transportation or purchasing of images of minors engaged in sexually explicit conduct;

5. Any and all address books, names, lists of names, telephone numbers, and addresses of individuals engaged in the transfer, exchange, or sale of child pornography;

6. Any non-digital recording devices and non-digital media capable of storing images and videos.

7. Digital devices and/or their components, which include, but are not limited to:

a. Any digital devices and storage device capable of being used to commit, further, or store evidence of the offense listed above;

b. Any digital devices used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, cameras, printers, encryption devices, and optical scanners;

- 1           c.     Any magnetic, electronic, or optical storage device capable of
- 2 storing data, such as disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, printer or
- 3 memory buffers, smart cards, PC cards, memory sticks, flashdrives, USB/thumb drives,
- 4 camera memory cards, media cards, electronic notebooks, and personal digital assistants;
- 5           d.     Any documentation, operating logs and reference manuals regarding
- 6 the operation of the digital device or software;
- 7           e.     Any applications, utility programs, compilers, interpreters, and other
- 8 software used to facilitate direct or indirect communication with the computer hardware,
- 9 storage devices, or data to be searched;
- 10          f.     Any physical keys, encryption devices, dongles and similar physical
- 11 items that are necessary to gain access to the computer equipment, storage devices or
- 12 data; and
- 13          g.     Any passwords, password files, test keys, encryption codes or other
- 14 information necessary to access the computer equipment, storage devices or data;
- 15        8.     Evidence of who used, owned or controlled any seized digital device(s) at
- 16 the time the things described in this warrant were created, edited, or deleted, such as logs,
- 17 registry entries, saved user names and passwords, documents, and browsing history;
- 18        9.     Evidence of malware that would allow others to control any seized digital
- 19 device(s) such as viruses, Trojan horses, and other forms of malicious software, as well
- 20 as evidence of the presence or absence of security software designed to detect malware;
- 21 as well as evidence of the lack of such malware;
- 22        10.    Evidence of the attachment to the digital device(s) of other storage devices
- 23 or similar containers for electronic evidence;
- 24        11.    Evidence of counter-forensic programs (and associated data) that are
- 25 designed to eliminate data from a digital device;
- 26        12.    Evidence of times the digital device(s) was used;
- 27        13.    Any other ESI from the digital device(s) necessary to understand how the
- 28 digital device was used, the purpose of its use, who used it, and when.

1           14. Records and things evidencing the use of the IP address 73.53.83.83 (the  
2 SUBJECT IP ADDRESS) including:

- 3           a. Routers, modems, and network equipment used to connect  
4 computers to the Internet;  
5           b. Records of Internet Protocol (IP) addresses used;  
6           c. Records of Internet activity, including firewall logs, caches, browser  
7 history and cookies, "bookmarked" or "favorite" web pages, search terms that the user  
8 entered into any Internet search engine, and records of user-typed web addresses.

9  
10 **The seizure of digital devices and/or their components as set forth herein is**  
11 **specifically authorized by this search warrant, not only to the extent that such**  
12 **digital devices constitute instrumentalities of the criminal activity described above,**  
13 **but also for the purpose of the conducting off-site examinations of their contents for**  
14 **evidence, instrumentalities, or fruits of the aforementioned crimes.**  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28